Compliance Component

DEFINITION

Name	Separation of duties
Description	Separation of duties is an organizational principle, which specifies that functions are assigned in a manner so that no one individual can control every activity in an end-to-end process.
Rationale	Provides process integrity while maintaining proper security and quality controls.

Benefits	• Having different staff engaged within an end-to-end process is a common, sensible business practice that ensures consistent and successful execution of the process.
	
	• Effective separation of duties provides for a system of checks and balances when following the general principles below:
	  • Separate system ownership from the system certification/accreditation process
	  • Separate system administration from system auditing.
	  • Separate operational responsibility from record keeping responsibility
	
	• Helps ensure "the fox isn't guarding the henhouse"
	
	NOTE: Adhering to these principles may not be possible due to resource limitations or other considerations. In these cases, the risk resulting from inadequate separation of duties should be assessed to ensure that the level of exposure is acceptable to an agency or division management.

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Management Controls
List the Technology Area Name	Personnel Security
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Separation-of-duties must be established and documented in order that an individual not have access to more than one critical task as identified by management. Examples of tasks that should be performed by different individuals: • Development

	• Testing • Administration (e.g. database, systems, network, etc.) • Physical security • IT security An audit policy should be established to ensure compliance with the separation-of-duties policy.
Document Source Reference #	International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management.

Standard Agency			
Name	Applying Security Practices to Justice Information Sharing	*Website*	http://it.ojp.gov/documents/asp/disciplines/index.htm
Contact Information			

Government Body			
Name	International Standard, ISO/IEC 17799, Information Technology—Code of Practice for Information Security Management. NIST SP800-12 An Introduction to Computer Security: The NIST Handbook.	*Website*	http://www.iso17799software.com http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
Contact Information			

KEYWORDS	
List all Keywords	Management, administration, policy, procedures, planning, staffing, critical tasks, sensitive, data.

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions	
Document the Conditional Use Restrictions	

Migration Strategy	
Document the Migration Strategy	

Impact Position Statement	
Document the Position Statement on Impact	

CURRENT STATUS				
Provide the Current Status)	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*
AUDIT TRAIL				
Creation Date	05/25/06	*Date Accepted / Rejected*	06/13/06	
Reason for Rejection				
Last Date Reviewed		*Last Date Updated*		
Reason for Update				